Managed Detection and Response (MDR)

Natica **MDR** hizmeti, müşterinin siber saldırılara karşı dayanıklılığını artırmayı ve olası tehditlere hızla yanıt vermeyi amaçlar. İki farklı hizmet modeli sayesinde, ihtiyaçlara ve bütçeye en uygun çözüm seçilebilir. Natica MDR hizmetleri, güvenlik operasyonlarını güçlendirirken, uzman deneyimi ve sürekli iyileştirme yaklaşımlarıyla riskleri minimuma indirmeye destek olur.

Neden MDR hizmetine ihtiyaç var?

Uzmanlık Eksikliği: Siber güvenlik alanında uzman bulmak ve elde tutmak zor ve maliyetli olabilir. **MDR** hizmeti, alanında uzman bir ekibe erişim sağlayarak bu sorunu ortadan kaldırır.

Sınırlı Kaynaklar: Güvenlik operasyonları için gerekli altyapıyı kurmak ve yönetmek zaman alıcı ve maliyetli olabilir. **MDR** hizmeti, bu yükü üzerinizden alarak kaynaklarınızı daha verimli kullanmanızı sağlar.

Gelişmiş Tehditler: Günümüzün siber saldırıları karmaşık ve sofistike hale geldi. MDR hizmeti, gelişmiş tehdit analizi ve proaktif tehdit avı ile bu saldırılara karşı koruma sağlar.

Sürekli İzleme: Siber saldırılar herhangi bir zamanda gerçekleşebilir. **MDR** hizmeti, 7/24 izleme ve müdahale sağlayarak kurumunuzu her zaman güvende olmasını sağlar.

Hizmet Modellerimiz

Natica, iş ortaklarının siber güvenlik ihtiyaçlarına yanıt verebilmek amacıyla iki farklı **MDR (Managed Detection and Response)** hizmet modeli sunar. Aynı zamanda tehditleri tespit etmek ve saldırılarla ilgili önleyici aksiyonları almak için EDR ya da NDR gibi güvenlik ürünlerini etkin olarak kullanır. Natica **MDR** hizmetiyle birlikte, **MDR** konusunda uzman kişiler tarafından alarmların incelenmesi, karantina aksiyonlarının alınması ve detaylı raporların oluşturulmasını sağlar.

Alarm Bazlı Talep Üzerinden MDR Hizmeti Modeli nedir?

Alarm bazlı talep Üzerinden **MDR Hizmeti Modelinde** müşteriden gelen alarm veya talebe bağlı olarak analiz ve raporlama yapılır:

- **Alarm Analizi:** Kurum içerisinde kullanılan EDR, NDR vb. güvenlik çözümleri ürünlerinde üretilen alarmlar detaylı olarak incelenir.
- **Tespit ve Önceliklendirme:** Olası güvenlik tehditleri veya şüpheli aktiviteler doğrulanır ve etki analizi yapılır.
- **Raporlama:** Hazırlanacak rapor içerisinde aşağıdaki konu başlıkları yer almaktadır.
  - Bulgular (tespit edilen zararlı aktiviteler, sistem açıkları vb.),
  - İyileştirme önerileri (konfigürasyon değişiklikleri, politika güncellemeleri, vb.),
  - Alınması gereken aksiyonlar (gerekirse ilgili sistemin karantinaya alınması gibi)

Alarm Bazlı Talep Üzerinden MDR Hizmeti Modeli müşteriye ne sağlar?

- Uzman analistler tarafından vaka bazlı tehdit analizi
- Kanıt odaklı raporlama ve aksiyon önerileri
- Talep üzerine karantina, ağda izolasyon (Containment) gibi hızlı müdahale gerektiren aksiyonlar

7/24 İzleme Temelli MDR Hizmeti Modeli nedir?

A7/24 İzleme Temelli **MDR Hizmeti Modelinde**, güvenlik ürünlerinin sürekli olarak (7/24) izlenmesi sağlanır:

- **Sürekli İzleme:** EDR, NDR vb. sistemlerinizde oluşan alarmlar ve tehdit göstergeleri, 7/24 uzmanlarımız tarafından takip edilir.
- **Proaktif Tehdit Avı:** Güncel tehdit istihbaratı ışığında proaktif savunma stratejileri geliştirilerek, düzenli aralıklarla gerçekleştirilen siber tehdit avı (threat hunting) faaliyetleri kapsamında, henüz belirgin bir alarm üretmeyen ancak sistemlerde potansiyel risk oluşturabilecek tehditlerin proaktif olarak tespit edilmesi hedeflenmektedir.
- **Çağrı Bazlı Analiz + Raporlama:** Birinci modelde sunulan tüm analiz ve raporlama hizmetlerini içerir.
- **Hızlı Müdahale:** Şüpheli veya zararlı faaliyet tespit edildiğinde; karantina, ağda izolasyon (Containment) gibi hızlı müdahale gerektiren aksiyonların alınması.

7/24 İzleme Temelli MDR Hizmeti Modeli müşteriye ne sağlar?

- 7/24 güvenlik izleme ve anlık alarm müdahalesi
- Tehdit avı (Threat Hunting) ve proaktif yaklaşım
- Detaylı bulgu raporları ve aksiyon önerileri

Hizmet Modellerimizin Karşılaştırılması

Özellik	Çağrı Bazlı Talep Üzerinden MDR Hizmeti	7/24 İzleme Temelli MDR Hizmeti
İzleme	8*5 (mesai saatleri içinde)	7/24
Tehdit Tespiti	Reaktif (müşteri talebine göre)	Proaktif (sürekli izleme ve tehdit avı)
Raporlama	Vaka bazlı	Düzenli

Neden Bizi Seçmelisiniz?

◆Uzman Ekip ◆Proaktif Yaklaşım ◆7/24 Destek ◆Özelleştirilebilir Hizmetler ◆Şeffaflık

Opsiyonel Saldırı Simülasyonu Testi

Natica MDR hizmeti öncesinde, müşteri tarafından talep edilmesi durumunda Picus, ThreatBlade veya muadili bir saldırı simülasyonu ürünü kullanılarak periyodik testler gerçekleştirilmektedir. Bu sayede, Natica MDR hizmetinde kullanılacak araçların ve süreçlerin ne kadar etkin çalıştığı gözlemlenebilir.

Saldırı simülasyonlarında farklı senaryolar (zararlı yazılım, dosyasız saldırılar, ağ zafiyetleri vb.) oynatılarak sistemlerin alarmlara nasıl tepki verdiği ölçülür.

Elde edilen sonuçlar doğrultusunda iyileştirme önerileri ve aksiyon planları hazırlanabilir.

www.natica.global natica@natica.global +90 (212) 296 61 90
Pasific Plaza A Blok Sevinçli Sok. N:3 K:8 Küçükbakkalköy Ataşehir 34750 İstanbul